Rechtsbescherming bij het gebruik van big data door toezichthouders: een verkenning

Gerrit-Jan Zwenne, Wilfred Steenbruggen & Michael Reker

Willen toezichthouders en bestuursorganen gebruikmaken van *big data predictive analytics*, dan moeten zij dit doen binnen de daarvoor geldende bestuursrechtelijke en privacyrechtelijke kaders. Zij krijgen te maken met rechtsvragen over beschikbaarheid en bruikbaarheid en – omdat er bij toezicht vrijwel altijd op enig moment sprake zal zijn van een verwerking van persoonsgegevens – de privacywetgeving. In dit artikel komen aan de orde over welke gegevens toezichthouders kunnen en mogen beschikken, welke conclusies zij op basis van big-data-analyses kunnen trekken en hoe in dit alles de belangen van rechtssubjecten kunnen worden gewaarborgd.

1 Inleiding

In dit tijdschrift is al eens ingegaan op het gebruik van *big data predictive analytics* door bestuursorganen en toezichthouders en de risico's daarvan.[1] In deze bijdrage bespreken wij in vogelvlucht enkele rechtsvragen die in elk geval moeten worden beantwoord als er bij toezichthouders de wens of behoefte is om in het kader van de een of andere toezichthoudende taak gebruik te maken van dergelijke analyses.

- Dat betreft allereerst vragen met betrekking tot de beschikbaarheid van de gegevens op basis waarvan de analyse is gedaan: in hoeverre kan een toezichthouder beschikken over de voor die analyse benodigde gegevens? Op basis van welke bevoegdheden kan en mag hij deze opvragen bij collega-toezichthouders of anderen? (par. 2)
- Vervolgens zijn er vragen over wat toezichthouders met deze analyses kunnen en mogen doen. Oftewel vragen naar de kwaliteit en betekenis van de uitkomsten van de analyses: welke conclusies kunnen op basis daarvan worden getrokken en welke gevolgen mogen daaraan dan worden verbonden? (par. 3)
- Ten slotte zijn er vragen over de rechtsbescherming van degenen over wie gegevens worden verwerkt: in hoeverre hebben zij kennis van de analyse van hun gegevens en welke mogelijkheden hebben zij dan om zich daartegen te verweren? (par. 4)

In deze bijdrage beperken wij ons daarbij vooral tot de big-data-analyses waarbij er sprake is van de verwerking van persoonsgegevens. In dergelijke gevallen is de privacywetgeving van toepassing en dat betreft thans de Wet bescherming persoonsgegevens en straks, vanaf 25 mei 2018 de Algemene Verordening Gegevens-

1 B.H. Custers, Risicogericht toezicht, profiling en Big Data, TvT 2014/5, p. 9-16.

bescherming[2] (AVG) en de Uitvoeringswet AVG.[3] Wij zijn ons ervan bewust dat wij daarmee het onderwerp van deze bijdrage misschien beperkt opvatten – er zijn talloze big-data-toepassingen waarbij het gaat om andere dan persoonsgegevens – maar wij denken dat dit in dit geval te billijken is, omdat er bij toezicht vrijwel altijd op enig moment sprake zal zijn van een verwerking van persoonsgegevens. En toch ook omdat de juridische discussies over big data vooralsnog vooral gaan over privacy en gegevensbescherming.[4]

Het belang van deze rechtsvragen houdt verband met de juridische houdbaarheid van de argumentatie die mede is gebaseerd op de uitkomsten van deze analyses. Een voorbeeld is de situatie waarin op basis van een big-data-analyse de Belastingdienst zou besluiten om iemands zorgtoeslag naar beneden bij te stellen, omdat het risicoprofiel van de desbetreffende belastingplichtige daartoe aanleiding geeft (argumentatie: 'in 84,3 procent van de vergelijkbare gevallen die zijn onderzocht blijkt er sprake te zijn van zorgfraude'). Als vervolgens wordt vastgesteld dat er bij de besluitvorming geen enkele betekenis is toegekend aan de op deze belastingplichtige van toepassing zijnde concrete omstandigheden, is er sprake van een onhoudbaar, vernietigbaar besluit (bijvoorbeeld vanwege het zorgvuldigheids- en evenredigheidsbeginsel of het vereiste van een deugdelijke motivering).

2 Over welke gegevens kan en mag een toezichthouder beschikken?

Veel toezichthouders hebben, naar eigen zeggen,[5] te maken met een veel te beperkte toezichtscapaciteit en moeten dus hun beperkte middelen zo veel mogelijk daar inzetten waar deze het meest effectief zijn. Om deze reden wordt vaak gekozen voor meer risicogericht toezicht – dat wil zeggen toezicht waarbij de prioriteit wordt gelegd bij de organisaties waar zich de grootste risico's voordoen. Voor de hand ligt dan het gebruik van profilering en big-data-analyse.

Een dergelijke analyse begint bij het verzamelen en bijeenbrengen van de daarvoor te gebruiken gegevens. Een eerste vraag is dan ook op basis van welke bevoegdheden toezichthouders dat kunnen doen en welke beperkingen ze daarbij in acht moeten nemen. In het verlengde daarvan ligt een tweede vraag, namelijk de vraag in hoeverre toezichthouders de op basis van hun bevoegdheden verkre-

2 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), 4 mei 2016, PbEU 2016, L 119/1.

3 Een ontwerp van de Uitvoeringswet AVG is eind 2016 ter consultatie aangeboden via <www.internetconsultatie.nl> (zoekwoord 'AVG').

4 Zie A. Lafarre, Recht voor big data, big data voor recht, Computerrecht 2016/3, p. 146-149.

5 Zie bijv. J. Kohnstamm, tot 1 augustus jl. de voorzitter van de Autoriteit Persoonsgegevens (AP), in een interview: 'Ik word altijd giechelend aangekeken als ik ervoor pleit ons budget te vervijfvoudigen, maar dat zou nog maar een begin zijn. We moeten nu te veel laten liggen', in: D. Tokmetzis & M. Martijn, Misschien moeten we het woord privacy niet meer gebruiken, zegt de man die er toezicht op hield, De Correspondent, 1 augustus 2016.

doi: 10.5553/TvT/187987052016007004003

gen gegevens met elkaar kunnen delen, en voor zover dat kan, onder welke voorwaarden. We bespreken de beide vragen.

2.1 Bevoegdheden om gegevens te verzamelen

De basis voor de bevoegdheden van toezichthouders om gegevens te kunnen verzamelen, wordt in de eerste plaats gevormd door titel 5.2 van de Algemene wet bestuursrecht (Awb), al dan niet in combinatie met de bijzondere wetten ten aanzien waarvan een bepaalde toezichthouder toezicht houdt op de naleving daarvan.

In deze titel van de Awb worden aan personen die bij of krachtens wettelijk voorschrift zijn belast met het houden van toezicht in de zin van artikel 5:11 Awb verschillende bevoegdheden toegekend om in te zetten ten behoeve van de uitoefening van hun wettelijke taken. Het gaat dan om het vorderen van inlichtingen (art. 5:16 Awb) of het vorderen van inzage van zakelijke gegevens en bescheiden, en de bevoegdheid om van deze gegevens en bescheiden kopieën te maken dan wel deze mee te nemen (art. 5:17 Awb). Daarbij is eenieder verplicht aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden (art. 5:20 lid 1 Awb). Dit biedt aan toezichthouders een krachtig middel om gegevens te verkrijgen. Wél geldt dat een toezichthouder slechts van deze bevoegdheden gebruik mag maken voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is (art. 5:13 Awb).

Eenmaal verzameld, zijn de gegevens in beginsel beschikbaar voor alle afdelingen van het bestuursorgaan dat de gegevens initieel heeft verzameld, voor zover zij die nodig hebben voor de uitoefening van hun wettelijke taken. Zo verkrijgt de afdeling binnen de Autoriteit Consument en Markt (ACM) die zich bezighoudt met handhaving van de Mededingingswet gegevens van diverse marktpartijen in het kader van het uitvoeren van een marktonderzoek (art. 6b lid 1 jo. art. 2 lid 2 en 4 Instellingswet ACM). Eenmaal verkregen kan de afdeling binnen ACM die zich bezighoudt met handhaving van de telecommunicatiewetgeving ook gebruikmaken van de verkregen gegevens, althans voor zover deze redelijkerwijs nodig zijn voor de uitoefening van haar in deze telecommunicatiewetgeving opgedragen wettelijke taken (art. 7 lid 1 Instellingswet ACM).[6]

Uit dit voorbeeld blijkt al dat er aan toezichthouders nogal eens uiteenlopende wettelijke taken zijn opgedragen. En ook dat er daardoor mogelijkheden ontstaan om de gegevens verkregen in het kader van de éne taak te gebruiken in het kader van een heel andere taak. We zien daar een spanningsveld met het evenredigheidsbeginsel (art. 5:13 Awb) en andere beginselen van behoorlijk bestuur, zoals het verbod van détournement de pouvoir (art. 3.3 Awb) of het daaraan verwante, in de privacywetgeving gehanteerde, doelbindingsvereiste (art. 9 lid 1 Wbp of art. 5 lid 1 sub b AVG). Het gaat er dan om dat een gegevensvorderingsbevoegdheid, en de met behulp daarvan verkregen gegevens, niet voor een ander doel wordt gebruikt dan waarvoor die bevoegdheid is bedoeld. Uiteraard moet het gebruik

6 Kamerstukken II 2012/13, 33622, 3, p. 46-47.

van een bevoegdheid niet worden verward met het gebruik van de gegevens die met zo een bevoegdheid is verkregen. Wél is het goed te onderkennen dat de mogelijkheid om gegevens voor een andere wettelijke taak te gebruiken, een risico kan betekenen dat van de desbetreffende bevoegdheid gebruik wordt gemaakt voor een ander doel dan waarvoor die is gegeven. In de volgende paragraaf, die gaat over het delen van gegevens met andere toezichthouders, wordt dat risico gearticuleerd.

2.2 Bevoegdheden om gegevens te delen

Onder voorwaarden kunnen de door één toezichthouder verkregen gegevens ook beschikbaar worden gesteld aan andere toezichthouders. Een dergelijke gegevensuitwisseling moet zijn voorzien bij of krachtens wet (zoals in een ministeriële regeling) en de ontvangende toezichthouder mag de verkregen gegevens alleen gebruiken voor doeleinden die bij of krachtens de desbetreffende wet zijn bepaald. Zo mag de Nederlandse Zorgautoriteit (NZa) op grond van de Wet marktordening gezondheidszorg (Wmg) (desgevraagd) gegevens en inlichtingen verstrekken aan een groot aantal toezichthouders en anderen, indien en voor zover die gegevens van belang kunnen zijn voor de uitoefening van hun wettelijke taken (art. 70 Wmg). Er kan dan worden verstrekt aan achtereenvolgens: het Zorginstituut, het College sanering, het Staatstoezicht op de volksgezondheid, ACM, De Nederlandsche Bank, de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP),[7] de FIOD-ECD, de Gezondheidsraad, het Rijksinstituut voor de volksgezondheid en milieu, de Raad voor de Volksgezondheid en Zorg, de Raad voor gezondheidsonderzoek, het Centraal Bureau voor de Statistiek en het Sociaal Cultureel Planbureau.

In de praktijk kiezen toezichthouders er veelal voor om de onderlinge gegevensuitwisseling nader uit te werken in samenwerkingsconvenanten of -protocollen. Zo hebben NZa en AFM een samenwerkingsconvenant[8] opgesteld ten behoeve van de onderlinge uitwisseling van gegevens in het kader van de uitoefening van hun wettelijke taken. En ACM heeft een samenwerkingsprotocol[9] gesloten met de Nederlandse Voedsel- en Warenautoriteit, waarin ook de onderlinge informatieuitwisseling is geregeld. In de praktijk bestaan er legio samenwerkingsverbanden, waardoor er een web van samenwerkingsarrangementen is ontstaan, met bijbehorende al dan niet structurele gegevensuitwisseling.

De onderlinge gegevensuitwisseling is niet onbeperkt en vindt haar begrenzing in de bij of krachtens de wet opgenomen beperkingen met betrekking tot de doeleinden waarvoor verkregen gegevens mogen worden gebruikt. Ook gelden de onverminderd de overige bestuursrechtelijke waarborgen, en dat zowel in de toezichtsfase als in de fase van een administratief sanctietraject. We noemden al het even-

7 Het College bescherming persoonsgegevens (Cbp) wordt, aldus art. 51 lid 4 Wbp, in het maatschappelijk verkeer aangeduid als: Autoriteit Persoonsgegevens (AP).

8 Samenwerkingsconvenant AFM-NZa, Stcrt. 2014, 4423.

9 Samenwerkingsprotocol tussen Autoriteit Consument & Markt en Nederlandse Voedsel- en Warenautoriteit, Stcrt. 2016, 44592.

doi: 10.5553/TvT/187987052016007004003

redigheidsbeginsel (art. 5:13 Awb). In de toezichtsfase verlangt dit beginsel dat geen inzage gevorderd wordt van andere documenten en bescheiden dan de bescheiden die verband houden met de wettelijke voorschriften waarop het toezicht in het concrete geval betrekking heeft. Dat betekent dat gegevens alleen mogen worden uitgewisseld voor zover deze relevant zijn in het kader van dat toezicht. In het sanctietraject kan gedacht worden aan de waarborgen die voortvloeien uit de onschuldpresumptie (art. 6 lid 2 EVRM), het zwijgrecht of de verplichting tot het geven van de cautie (art. 5:10a Awb).[10] Deze waarborgen brengen onder meer met zich mee dat documenten die specifiek worden opgesteld en verstrekt in het kader van bijvoorbeeld een marktonderzoekstraject, niet zomaar mogen worden verstrekt aan een andere toezichthouder ten behoeve van de bewijsvoering in een administratief sanctietraject. Bovendien geldt dat elke gegevensuitwisseling slechts mag plaatsvinden als de geheimhouding van de betreffende gegevens door de ontvangende toezichthouder in voldoende mate is gewaarborgd (art. 2:5 Awb) en dat voldoende is gewaarborgd dat de ontvangende toezichthouder de gegevens niet zal gebruiken voor een ander doel dan waarvoor de gegevens worden verstrekt.[11]

In aanvulling op deze bestuursrechtelijke waarborgen geldt dat de onderlinge gegevensuitwisseling binnen de organisatie van een toezichthouder en tussen toezichthouders ook moet voldoen aan de vereisten voortvloeiend uit de privacywetgeving, voor zover de bij de uitoefening van een bepaalde wettelijke taak verkregen gegevens kwalificeren als persoonsgegevens.[12] In dat geval moet de uitwisseling van gegevens worden beschouwd als een verdere verwerking van persoonsgegevens. Op grond van artikel 9 lid 1 Wbp is een dergelijke verdere verwerking niet toegestaan als deze onverenigbaar is met de doeleinden waarvoor deze gegevens oorspronkelijk zijn verkregen. Ook is verdere verstrekking niet toegestaan als geheimhoudingsverplichtingen uit hoofde van ambt, beroep of wettelijk voorschrift zich daartegen verzetten.[13]

Extra regels gelden als de persoonsgegevens kwalificeren als bijzondere gegevens (art. 16 Wbp). Daaronder vallen onder andere strafrechtelijke persoonsgegevens, zoals vastgestelde overtredingen of vermoedens van 'min of meer gegronde verdenkingen'.[14] Voor dergelijke persoonsgegevens geldt in beginsel een verwerkingsverbod, waarop alleen uitzonderingen mogelijk zijn als er sprake is van een van de uitzonderingen van artikel 22 en 23 Wbp of als een bijzondere wet (*lex specialis*) voorziet in een wettelijke bevoegdheid daartoe.[15]

10 Vgl. ook: Kamerstukken I 2012/13, 33186, D, p. 3-4; CBb 2 februari 2010, ECLI:NL:CBB:2010:BL5463; CRvB 1 augustus 2014, ECLI:NL:CRVB:2014:2607; CRvB 21 juli 2015, ECLI:NL:CRVB:2015:2451; Rb. Rotterdam 16 september 2016, ECLI:NL:RBROT:2016:3582.

11 Ibid.

12 Art. 1 sub f Wbp definieert persoonsgegevens als de gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Oftewel gegevens over mensen van wie de identiteit bekend is of zonder onevenredige inspanning bekend kan worden.

13 Zie in dit verband: Kamerstukken II 2011/12, 33186, 6, p. 41.

14 Kamerstukken II 1997/98, 25892, 3, p. 118.

15 Kamerstukken II 1997/98, 25892, 3, p. 43.

Een expliciete wettelijke bevoegdheid tot gegevensverkrijging of informatie-uitwisseling (zoals art. 70 Wmg) geldt als *lex specialis* ten opzichte van de Wbp. Bij het ontbreken daarvan kan voor de uitwisseling van strafrechtelijke persoonsgegevens met andere toezichthouders soms ook gebruik worden gemaakt van de uitzondering in artikel 22 lid 6 Wbp. Daarin is bepaald dat het verwerkingsverbod niet van toepassing is op verwerkingen van strafrechtelijke gegevens door en ten behoeve van publiekrechtelijke samenwerkingsverbanden, als (1) de verwerking noodzakelijk is voor de uitvoering van de taak van de deelnemers aan het samenwerkingsverband én (2) als bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Daarnaast kan in voorkomende gevallen een beroep worden gedaan op de uitzonderingsgrond van een zwaarwegend algemeen belang in combinatie met een door AP verleende ontheffing (art. 23 lid 1 sub f Wbp). Ook daarvoor geldt een aantal voorwaarden: (1) er moet een zwaarwegend algemeen belang zijn, (2) de verwerking moet nodig zijn met het oog op dat zwaarwegende algemeen belang, en (3) er moeten passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer van de betrokkenen. Deze uitzonderingsgrond is in de praktijk evenwel vaak minder bruikbaar, omdat AP in voorkomende gevallen wel het standpunt heeft ingenomen dat een ontheffing slechts mogelijk is bij uitzicht op een wettelijke regeling waarin de verwerking van bijzondere gegevens wordt geregeld. Er moet dan dus, volgens AP, een wetsvoorstel in de maak zijn dat deze gegevensverwerking mogelijk gaat maken.[16]

Het voorgaande maakt duidelijk dat toezichthouders ruime maar uiteraard niet onbegrensde bevoegdheden hebben om gegevens te verzamelen en voorts dat zij deze gegevens veelal ook met andere toezichthouders mogen delen. Dat creëert mogelijkheden voor het bijeenbrengen van veel gegevens en het vervolgens inzetten van big-data-analyses in en en behoeve van het toezicht. Van big data en profilering wordt, misschien niet ten onrechte, door toezichthouders ook veel verwacht. Toch is er aanleiding om het gebruik van big data in het toezicht met de nodige terughoudendheid tegemoet te treden. Deze inzet is namelijk niet onproblematisch.

3 Welke conclusies kunnen op basis van big-data-analyses worden getrokken?

De term big data wordt in veel verschillende betekenissen gebruikt.[17] De gemeenschappelijke deler is dat het gaat om het verzamelen en gebruiken van 'grote' gegevensverzamelingen of datasets, bestaande uit gegevens uit diverse bronnen

16 Of dit vast beleid is van de toezichthouder is overigens de vraag. In ABRvS 3 september 2008, ECLI:NL:RVS:2008:BE9698 verdedigde de toezichthouder *nota bene* zelf dat de ontheffing voor een pilotproject in casu wel kon worden verleend omdat deze nodig was om te bepalen of een wettelijke regeling wel of niet nodig was.

17 Zie voor een overzicht WRR 2016, p. 33 e.v.

Tijdschrift voor Toezicht 2016 (7) 4
doi: 10.5553/TvT/187987052016007004003

die niet altijd eenvoudig doorzoekbaar of koppelbaar zijn. De desbetreffende gegevensverzamelingen laten zich hierdoor lastig gericht, op basis van vooraf opgestelde hypotheses en vraagstellingen, doorzoeken. Daarom wordt met complexe zoekalgoritmes gezocht naar mogelijk interessante verbanden en patronen in de data. Dit kan allerlei statistische verbanden of correlaties opleveren die soms nog niet goed verklaarbaar zijn of nog niet aantoonbaar causaal zijn, maar wel voorspellende waarde hebben en kunnen worden vertaald naar risico- of andersoortige profielen.

We zijn er inmiddels mee vertrouwd dat aan dergelijke profielen betekenis kan worden toegekend en deze daarmee waardevol zijn. In de private sector kennen we verschillende voorbeelden van organisaties die op basis van aankoopgegevens of gegevens over wat wij doen op internet (surfgedrag) klant- of gebruikersprofielen opstellen aan de hand waarvan ze vervolgens gerichte aanbiedingen kunnen doen ('behavorial advertizing' of 'behavorial targeting').[18] Al wat langer kennen we de risicoprofielen met betrekking tot kredietwaardigheid en betalingsgedrag ('credit score') op basis waarvan wordt bepaald of klanten al dan niet in aanmerking komen voor een krediet of voor een bepaalde betaalwijze (denk aan: kopen op afbetaling). Van sommige vliegmaatschappijen wordt wel gezegd dat op basis van dergelijke profielen de door een klant te betalen ticketprijs wordt gepersonaliseerd, wat naar verluidt met zich kan brengen dat de gebruikers van dure computers (zeg: een Apple Macbook) een hogere prijs betalen dan degenen die gebruikmaken van een goedkopere Windows PC.[19]

Ook van verschillende toezichthouders is bekend dat zij, veelal in samenwerkingsverbanden met andere toezichthouders en instanties, gebruikmaken van data-analyses en risicoprofielen om hun beperkte toezichtscapaciteit gerichter en dus effectiever te kunnen inzetten. Zo maakt de Belastingdienst bijvoorbeeld al gebruik van data-analyses om belastingfraude te kunnen opsporen,[20] de politie zoekt naar hotspots en veelplegers om preventief misdaad te bestrijden,[21] gemeenten, UWV en andere instanties maken gebruik van het Systeem Risico Identificatie (SyRI) om risicoanalyses uit te voeren met het oog op de opsporing van sociale zekerheidsfraude,[22] de Marechaussee kijkt naar opvallende reisbewegingen van voertuigen of personen en financiële toezichthouders kijken naar

18 Zo kon de Amerikaanse supermarkt Target aan de hand van een dergelijke analyse voorspellen of iemand zwanger was en daarop inspelen door aanbiedingen. Zie C. Duhigg, How Companies Learn Your Secrets, New York Times, 16 februari 2012. Zie ook uitgebreid over behavorial targeting: F. Zuiderveen Borgesius, Improving Privacy Protection in the Area of Behavioural Targeting, Deventer: Kluwer Law International 2015.

19 J. Angwin & D. Mattioli, Coming Soon: Toilet Paper Priced Like Airline Tickets, Wall Street Journal, 2 september 2012. Over personalised pricing zie ook OFT, Personalised Pricing, May 2013, OFT 1489.

20 P. Olsthoorn, Big Data voor Fraudebestrijding, WRR: Den Haag 2016.

21 Zie D. Willems & R. Doelemans, Predictive Policing – wens of werkelijkheid?, Tijdschrift voor de Politie 2014-4/5, p. 39 e.v.

22 P. Olsthoorn, Big Data voor Fraudebestrijding, WRR: Den Haag 2016, p. 99 e.v.; zie over SyRI ook G-J. Zwenne & A.H.J. Schmidt, Wordt de homo digitalis bestuursrechtelijk beschermd?, in: Homo Digitalis, NJV-preadvies 2016, Deventer: Kluwer 2016, p. 310 en 339-341.

afwijkende transacties, boven een bepaald bedrag of naar een bepaald land, om te bepalen hoe en waar zij hun toezichtsbevoegdheden inzetten,[23] en ook in de zorg wordt door de NZa en zorgverzekeraars steeds meer gebruikgemaakt van data-analyses in de strijd tegen zorgfraude.[24]

Dat het gebruik van big data voor toezichthouders aantrekkelijk is, is wel duidelijk. Toezichthouders beschikken vaak al over heel veel, soms zeer gedetailleerde, data over het gedrag van mensen. Als zij deze data 'slim' kunnen gebruiken, stelt dat hen in staat om gerichter en effectiever te werken en zo veel tijd en geld te besparen. Maar dat laat onverlet dat juist toezichthouders zorgvuldig te werk zouden moeten gaan bij de analyse en het gebruik van big data. Ook big data kennen namelijk hun beperkingen. Wij noemen de belangrijkste:

- In de eerste plaats is er het biasprobleem. Gegevens worden altijd in een specifieke context verzameld. Daardoor zit in bijna iedere dataset een specifieke bias. Als die niet wordt gecorrigeerd, kan dat makkelijk leiden tot onjuiste of anderszins problematische uitkomsten. Wanneer de politie bijvoorbeeld enkel in wijken met veel allochtonen ('mensen met een migrantenachtergrond') surveilleert, zullen politiedatabanken vooral gevuld zijn met juist dergelijke personen. En dat zal doorwerken in de gemodelleerde risicoprofielen die dan onevenredig veel van deze allochtonen bevatten. Vooral bij het combineren en hergebruiken van databronnen kan het lastig zijn om te achterhalen hoe de datasets tot stand zijn gekomen en wat dus de precieze bias is die in data zit.
- Het is in de tweede plaats van belang te beseffen dat de verbanden die met behulp van big-data-analyses worden gelegd, niet noodzakelijk causaal van aard zijn. Het gaat om correlaties, dat wil zeggen om statistische verbanden. En dat maakt dat het enkele feit dat iemand past binnen een profiel nog niet automatisch betekent dat hij dus ook het aan dat profiel gekoppelde gedrag zal vertonen. Het verband kan ook indirect zijn of zelfs berusten op louter toeval. Zonder een betrouwbare theoretische basis over het hoe en waarom van de gevonden correlaties, en zonder goede aanwijzingen dat de verbanden causaal van aard zijn, kunnen daarop gebaseerde interventies de plank volledig misslaan, met grote consequenties.
- In de derde plaats zijn profielen, en dat geldt ook voor profielen die zijn opgesteld op basis van big data predictive analytics, sowieso altijd een benadering van de werkelijkheid en bevatten zij dus foutmarges. Het gevaar bestaat daarmee dat op basis van profielen de verkeerde conclusies worden getrokken, bijvoorbeeld omdat ten onrechte wordt aangenomen dat iemand binnen het profiel valt of juist niet. Dat sprake is van een foutmarge is voor het aanraden van een boek op Amazon of een film op Netflix niet erg. Maar het wordt wel problematisch als iemand op basis van analyses bijvoorbeeld ten onrechte op

23 B.H. Custers, Risicogericht toezicht, profiling en Big Data, TvT 2014/5, p. 9-16.
24 P. Olsthoorn, Big Data voor Fraudebestrijding, WRR: Den Haag 2016, p. 39 e.v.

Tijdschrift voor Toezicht 2016 (7) 4
doi: 10.5553/TvT/187987052016007004003

een no fly-list wordt gezet zoals de Amerikaanse senator Ted Kennedy[25] of Europees Parlementariër Sophie in 't Veld overkwam.[26]

– In de vierde plaats kunnen ook de data zelf onvolledig of onjuist zijn, met als gevolg dat ook de op basis daarvan bepaalde risicoprofielen onjuist zijn. Het werken met risicoprofielen vereist dat profielen voortdurend worden geactualiseerd. Profielen raken namelijk na verloop van tijd 'uitgewerkt', bijvoorbeeld omdat iedereen die aan het profiel voldoet, wordt aangepakt of omdat personen hun gedrag aanpassen en daardoor buiten het profiel vallen.[27]

Het voorgaande maakt duidelijk dat het gebruik van big data de nodige risico's kent die geadresseerd moeten worden, wil het gebruik daarvan juridisch aanvaardbaar zijn en als basis voor besluitvorming kunnen worden gebruikt. Zo is het niet moeilijk in te zien dat onzorgvuldig gebruik van big data als basis voor de inzet van toezichtsbevoegdheden op gespannen voet kan staan met de algemene beginselen van behoorlijk bestuur die onverkort gelden in het kader van het handhavingstoezicht en het boeteonderzoek. Het verbod op willekeur en het formele zorgvuldigheidsbeginsel (art. 3:4 lid 1 Awb) brengen met zich dat toezichthouders bij de inzet van hun bevoegdheden zorgvuldig te werk moeten gaan, ook als de toezichts- en boeteonderzoekhandelingen geen besluit zijn (vgl. art. 3:1 lid 2 jo. 3:2 Awb). Dat betekent wat ons betreft bijvoorbeeld dat toezichthouders die big data willen gebruiken, ervoor moeten zorgen dat zij beschikken over de voor hun doeleinden benodigde gegevens en dat deze van voldoende kwaliteit zijn. Daarnaast zullen zij ervoor moeten zorgen dat zij beschikken over de nodige expertise om goede analyses uit te voeren en de uitkomsten op een passende en controleerbare wijze te duiden.

Er is ook op meer principiële gronden aanleiding voor een terughoudend en zorgvuldig gebruik van big data en profilering door toezichthouders. Er zijn verschillende voorbeelden beschreven waarbij big data aanleiding gaven tot ongewenste discriminatie en stigmatisering. Big data maken het mogelijk om mensen in te delen in groepen op basis van eigenschappen, voorkeuren en activiteiten en ze op basis daarvan anders te behandelen. De computer maakt daarbij geen morele afweging. Het kan dus voorkomen, ook wanneer dat niet wordt beoogd, dat profielen niettemin de facto worden opgesteld op basis van etnische afkomst, religie en politieke voorkeur, wat op gespannen voet staat met het discriminatieverbod van artikel 1 van de Grondwet en de Algemene wet gelijke behandeling.

Die mogelijkheid is temeer reëel, omdat discriminatie ook als bias verscholen kan zitten in de correlatie, de dataset of het algoritme. Als er, voortbouwend op het eerdere voorbeeld, veel allochtonen voorkomen in de datasets, kunnen deze op extra aandacht rekenen van de politie, wat er weer toe kan leiden dat meer van hen in de databanken worden opgenomen. En als dit soort profielen bekend wordt bij een breder publiek kunnen ze ook stigmatiserende en discriminerende

25 V. Mayer-Schonberger & K. Cukier, Big data, Boston: Mariner Books 2014, p. 166-167.
26 E. Nakashima, European Lawmaker to Sue U.S. Over Data, Washington Post, 1 juli 2008.
27 B.H. Custers, Risicogericht toezicht, profiling en Big Data, TvT 2014/5, p. 12.

effecten hebben.[28] Het White House rapport over big data waarschuwt ook specifiek voor dit risico: 'The increasing use of algorithms to make eligibility decisions must be carefully monitored for potential discriminatory outcomes for disadvantaged groups, even absent discriminatory intent.'[29]

Het is van belang dat toezichthouders zich bewust zijn van het gevaar van discriminatie en passende maatregelen nemen om dit te voorkomen.

Big-data-processen zetten daarnaast de onschuldpresumptie onder druk en raken daarmee aan het recht op een eerlijk proces dat onder meer is gewaarborgd in artikel 6 EVRM.[30] Een aspect van de onschuldpresumptie is dat opsporingsbevoegdheden niet zomaar jegens eenieder mogen worden toegepast, maar dat er een redelijk vermoeden van het plegen van een strafbaar feit moet zijn of ten minste aanwijzingen voor de betrokkenheid bij strafbare feiten. Aan de verdachte komt bovendien een beschermde status toe om een eerlijk proces te waarborgen (denk aan het zwijgrecht en andere rechten die voortvloeien uit het *nemo tenetur*-beginsel, de inzage in processtukken en *equality of arms*). Deze waarborgen gelden uiteraard ook in het bestuursstrafrecht.[31] Degene die op basis van een data-analyse tot een risicogroep behoort die bijzondere aandacht krijgt, heeft die speciale status vaak (nog) niet en kan zich dus niet hiertegen verweren, als hij daarvan al op de hoogte is. Daarbij komt dat diegene ook vaak helemaal niet weet hoe de algoritmes, computersystemen en profielen werken, zodat een effectieve verdediging sowieso lastig is, ook nadat hij in een later stadium alsnog tot verdachte is 'gepromoveerd'. Dit maakt het eens te meer van belang dat toezichthouders zorgvuldig omgaan met big data en niet zomaar op basis daarvan overgaan tot de inzet van ingrijpende bevoegdheden of het opleggen van sancties.

Ook uit het privacyrecht volgt dat big data en profilering niet zonder meer als basis voor toezichtshandelen kunnen worden gebruikt. Dat geldt in ieder geval als profielen worden gebruikt als beslisinstrument. Artikel 42 lid 1 Wbp bepaalt dat niemand kan worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking van persoonsgegevens. Deze bepaling keert terug in artikel 22 lid 1 AVG dat nog eens expliciet aangeeft dat dit recht om niet te worden onderworpen aan volledig geautomatiseerde besluitvorming ook geldt bij profilering. Het is op grond hiervan dus in beginsel niet mogelijk om iemand uitsluitend op basis van een profiel te sanctioneren.

28 B. Custers, T. Calders, B. Schermer & T. Zarsky (red.), Discrimination and Privacy in the Information Society, Heidelberg: Springer 2013.

29 White House 2014, p. 47.

30 M. Hildebrandt, Data-gestuurde intelligentie in het strafrecht, in: Homo Digitalis, NJV-preadvies 2016, Deventer: Kluwer 2016, p. 188 e.v.

31 Zie bijv. R. Stijnen, Rechtsbescherming tegen bestraffing in het strafrecht en het bestuursrecht, Deventer: Kluwer 2011.

Tijdschrift voor Toezicht 2016 (7) 4
doi: 10.5553/TvT/187987052016007004003

Minder duidelijk is in hoeverre big data kunnen worden gebruikt als selectie-instrument voor de inzet van toezichtsbevoegdheden. Die vraag wordt met name relevant als het gaat om de inzet van een ingrijpende toezichtsbevoegdheid, bijvoorbeeld een bedrijfsbezoek of doorzoeking (bijv. art. 50 Mededingingswet). Het lijkt ons verdedigbaar dat bij de inzet van een dergelijke bevoegdheid sprake is van een beslissing die de betrokkene aanmerkelijk treft, zodat artikel 22 lid 1 AVG zich ertegen verzet dat deze enkel wordt gebaseerd op de uitkomst van een big-data-analyse.

Bij wet kan overigens wel een ruimer gebruik van geautomatiseerde besluitvorming op basis van profilering worden toegestaan, mits wordt voorzien in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene (zie art. 42 lid 2 sub b Wbp en art. 22 lid 2 sub b AVG). Wat die passende maatregelen zijn, is niet helemaal duidelijk, maar het zal daarbij in ieder geval gaan om maatregelen met het oog op rechtsbescherming.[32] Ook staat het privacyrecht er op zichzelf niet aan in de weg dat big data en profilering worden gebruikt ter *ondersteuning* van de besluitvorming, mits overigens aan de eisen van het privacyrecht is voldaan.
Het voorgaande maakt duidelijk dat toezichthouders om diverse redenen terughoudend en zorgvuldig te werk moeten gaan bij het gebruik van big data en profilering.

4 Hoe zit het met de rechtsbescherming van betrokkenen?

Het gebruik van big data door toezichthouders kent dus de nodige haken en ogen. Dat maakt het van belang dat er een effectieve rechtsbescherming is tegen besluitvorming op basis van big data en risicoprofielen. Hoe zit het daarmee? Kunnen betrokkenen effectief opkomen tegen het gebruik van big data door toezichthouders in bijvoorbeeld het kader van een boetetraject?

In de literatuur wordt er wel op gewezen dat rechtsbescherming problematisch is, omdat big-data-analyses zich vaak in eerste instantie niet richten op specifieke individuen, terwijl het recht daarentegen voornamelijk inzet op individuele rechtsbescherming.[33] In dat verband wordt wel bepleit dat privacy meer als een maatschappelijke of collectieve waarde zou moeten worden gezien en ook als zodanig beschermd moet worden. Daar valt wat ons betreft wel wat voor te zeggen. Individuen die geen last hebben van het gebruik van hun gegevens in een big-data-analyse, bijvoorbeeld omdat ze buiten het aan de hand daarvan opgestelde

32 Vgl. overweging 71 AVG: 'In ieder geval moeten voor dergelijke verwerking passende waarborgen worden geboden, waaronder specifieke informatie aan de betrokkene en het recht op menselijke tussenkomst, om zijn standpunt kenbaar te maken, om uitleg over de na een dergelijke beoordeling genomen besluit te krijgen en om het besluit aan te vechten.'

33 Zie bijv. B. van der Sloot, The Individual in the Big Data Era: Moving towards an Agent-Based Privacy Paradigm, in: B. van der Sloot e.a. (red.), Exploring the boundaries of Big Data, Amsterdam: Amsterdam University Press 2016, p. 177-203. Zie ook WRR, Big Data in een vrije samenleving, Amsterdam: Amsterdam University Press 2016, p. 114 e.v.

risicoprofiel vallen, zullen niet opkomen tegen de (vaak geringe) schendingen van hun privacy, als ze daar al achter komen. Een effectieve rechtsbescherming vraagt dan om een meer systeemgerichte aanpak waarbij meer nadruk ligt op de randvoorwaarden voor het gebruik van big data.

Het ligt voor de hand daarbij aansluiting te zoeken bij de in de rechtspraak door het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de EU (HvJ EU) ontwikkelde randvoorwaarden voor de inzet van heimelijke surveillance en grootschalige gegevensverwerking.[34] Dat betekent in de eerste plaats dat het gebruik van big data moet zijn terug te voeren op een wettelijke grondslag die duidelijke en precieze regels over de inzet van dit instrument bevat, zodat duidelijk is wanneer toezichthouders (ingrijpende) bevoegdheden kunnen inzetten op basis van big data. Deze regels zouden ook waarborgen moeten bevatten om misbruik van de gegevens te voorkomen en ervoor te zorgen dat alleen van big-data-analyse gebruik wordt gemaakt als dat nodig en proportioneel is. Ook zou met het oog op een effectieve rechtsbescherming moeten zijn voorzien in een onafhankelijk en effectief toezicht op het gebruik van big data, zodat ook wordt gecontroleerd of de inzet van big data voldoet aan de genoemde regels en bovendien of deze inzet met het oog op de in paragraaf 3 genoemde risico's verantwoord is.

Wij hebben onze twijfels of de huidige inzet van big data door toezichthouders wel in alle gevallen voldoet aan deze randvoorwaarden. Vaak is er wel een wettelijke grondslag voor de verzameling en uitwisseling van gegevens tussen toezichthouders, maar deze bevat veelal geen regels, laat staan duidelijke en precieze regels, voor de koppeling van datasets en de verdere analyse daarvan. Soms maken toezichthouders in een convenant nadere afspraken over de uitwisseling en het gebruik van gegevens, maar ook voor deze convenanten geldt dat het vaak beperkt blijft tot globale en weinig precieze afspraken over de onderlinge uitwisseling van gegevens.[35] Onafhankelijk toezicht op het gebruik van big data, bijvoorbeeld door middel van de aanstelling van een functionaris voor gegevensbescherming (ook wel *data protection officer* of DPO) of een onafhankelijke privacycommissie, maakt van deze afspraken in de meeste gevallen nog geen onderdeel uit.

34 Zie voor rechtspraak van het HvJ EU en EHRM bijvoorbeeld G-J. Zwenne & W.A.M. Steenbruggen, Privacyvoorwaarden voor de iOverheid. Vuistregels voor wet- en regelgevers met betrekking tot overheidsinformatiesystemen, Regelmaat 2015/1, p. 19-36, alsmede G-J. Zwenne & F. Simons, Daar kon je op wachten: richtlijn bewaarplicht ongeldig verklaard, Tijdschrift voor Internetrecht 2014-3, p. 70 e.v. Zie ook recent HvJ EU 21 december 2016, gevoegde zaken C-203/15 en C-698/15, Tele2 Sverige, ECLI:EU:C:2016:970 en EHRM 4 december 2015, nr. 47143/06, Roman Zakharov, Computerrecht 2016-86, m.nt. S.J. Eskens. Een uitgebreider, maar al wat ouder overzicht van relevante rechtspraak is te vinden in W.A.M. Steenbruggen, Publieke dimensies van privé-communicatie, Amsterdam: Otto Cramwinckel 2009, p. 81.

35 Zie bijv. het Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen, <www.riec.nl/oostbrabant/wet-en-regelgeving/nieuw-riec-convenant>.

Tijdschrift voor Toezicht 2016 (7) 4
doi: 10.5553/TvT/187987052016007004003

Wat daarvan verder ook zij, voor zover het gebruik van big data uitmondt in een besluit als bedoeld in de Awb, kan de betrokkene de big-data-analyse in ieder geval in dat verband aan de orde stellen. Dat kan in beginsel al in de fase van voorbereiding van het besluit. Een belanghebbende moet immers in de gelegenheid worden gesteld om een zienswijze te geven, indien de beschikking mede zou steunen op gegevens over feiten en belangen die de belanghebbende betreffen en die gegevens niet door hemzelf zijn verstrekt (art. 4:7 en 4:8 Awb).

Uit de parlementaire geschiedenis bij de Wbp blijkt dat de wetgever de artikelen 4:7 e.v. Awb als passende waarborgen ziet waarmee kan worden voorkomen dat beslissingen uitsluitend op basis van een langs geautomatiseerde weg tot stand gekomen beeld worden genomen.[36] Ook de AVG stelt als voorwaarde voor volledig geautomatiseerde besluitvorming dat de betrokkene het recht heeft op menselijke tussenkomst van de verantwoordelijke en dat hij zijn standpunt kenbaar kan maken en het besluit kan aanvechten (zie art. 22 lid 3 AVG).

De Awb lijkt hier evenwel verder te gaan dan de privacywetgeving, gelet op het feit dat de artikelen 4:7 en 4:8 Awb ook gelden als geen sprake is van volledig geautomatiseerde besluitvorming. Daarnaast gelden deze bepalingen ook als de belanghebbende geen natuurlijke persoon is. In de praktijk blijkt evenwel dat bestuursorganen in de fase van voorbereiding van het besluit nog wel eens afzien van het horen van een belanghebbende. De artikelen 4:11 en 4:12 Awb bieden daartoe enige ruimte, bijvoorbeeld ingeval de vereiste spoed zich tegen het horen verzet of het beoogde doel het horen in de weg staat. Daarnaast kan, mocht blijken dat ten onrechte niet is gehoord, dit gebrek bovendien in beginsel worden hersteld in de bezwaarprocedure.[37]

In een boetetraject kan het bestuursorgaan in ieder geval niet afzien van het horen van de belanghebbende als voor de overtreding een bestuurlijke boete van meer dan 340 euro kan worden opgelegd (art. 5:53 Awb). De belanghebbende moet dan in de gelegenheid worden gesteld zijn zienswijze te geven op het voornemen om een boete op te leggen en de gronden waarop dat berust (vgl. art. 5:48 Awb). Als dit voornemen mede is gebaseerd op een big-data-analyse, moet hij in beginsel ook daarop zijn zienswijze kunnen geven.

Problematisch is wel dat de belanghebbende vaak niet weet welke gegevens de toezichthouder in zijn analyse heeft betrokken en waar deze vandaan komen. Ook weet hij in de regel niet hoe de gebruikte algoritmes, computersystemen en profielen precies werken. Of een toezichthouder bereid is inzicht te geven in de big-data-analyses is daarbij de vraag, al was het maar omdat dit ten koste kan gaan van de effectiviteit van het daarop gebaseerde toezicht. Als bekend wordt hoe het profiel werkt, is er het risico dat degenen op wie het toezicht is gericht hun gedrag daarop aanpassen, waardoor de bruikbaarheid van het profiel wordt verminderd. Een en ander impliceert dat belanghebbenden ten opzichte van toezichthouders

36 Kamerstukken II 1997/98, 25892, nr. 3, p. 170.
37 MvT Parl. Geschiedenis AWB I, p. 256.

een kennisachterstand hebben die hen belemmert in hun mogelijkheden om zich te verweren tegen besluitvorming die mede op basis van big data plaatsvindt.[38]

Vastgesteld moet worden dat de Awb geen harde verplichting voor het bestuursorgaan bevat om de belanghebbende volledig en nauwkeurig te informeren over de big-data-analyse en de onderliggende logica. De Awb geeft de belanghebbende weliswaar in bezwaar en beroep een aanspraak op toegang tot het dossier, maar die toegang is niet onbeperkt, zeker niet buiten een boetetraject. Als gewichtige redenen dat rechtvaardigen, en dat kan het geval zijn als de effectiviteit van het toezicht op het spel staat, kunnen toezichthouders besluiten om het dossier slechts gedeeltelijk vrij te geven (vgl. art. 7:4 lid 6, Awb en art. 8:29 Awb). In een boetetraject heeft de belanghebbende in beginsel wel recht op het volledige dossier. Op grond van artikel 5:49 Awb dient het bestuursorgaan de belanghebbende in de gelegenheid te stellen alle gegevens in te zien waarop (het voornemen tot) het opleggen van de bestuurlijke boete berust. Maar dat betekent nog niet dat de belanghebbende daarmee ook volledig toegang krijgt tot de onderliggende big data-analyse en de logica daarachter. Dat hoeft in ieder geval niet als de big-data-analyse niet wordt gebruikt voor de bewijsvoering van de overtreding of de bepaling van de strafmaat.[39]

De privacywetgeving lijkt hier meer rechtsbescherming te kunnen bieden. Op grond van artikel 33 en 34 Wbp dient de verantwoordelijke de betrokkene in de eerste plaats actief te informeren over de verwerking van zijn persoonsgegevens. De verantwoordelijke moet op grond hiervan de betrokkene in ieder geval zijn identiteit mededelen en de doeleinden van de verwerking. Daarnaast moet hij de betrokkene nadere informatie verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen en het gebruik dat daarvan wordt gemaakt, nodig is om tegenover de betrokkene een zorgvuldige verwerking te waarborgen. Het lijkt goed verdedigbaar dat de verantwoordelijke de betrokkene op grond hiervan inzicht moet verschaffen in het hoe en waarom van de big-data-analyse. Die informatie moet de verantwoordelijke de betrokkene in ieder geval geven als hij daarom vraagt. Artikel 35 lid 4 Wbp bepaalt namelijk dat de verantwoordelijke desgevraagd mededelingen doet omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van gegevens betreffende de betrokkene.

De AVG gaat zelfs nog wat verder. Op grond daarvan moet de verantwoordelijke namelijk de betrokkene onder meer, actief of op diens verzoek, informeren over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en hem nuttige informatie verstrekken over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene (vgl. art. 13 lid 2 sub f, art. 14 lid 2 sub g en art. 15 lid 1 sub h AVG). Die informatie moet

38 Zie ook WRR, Big Data in een vrije samenleving, Amsterdam: Amsterdam University Press 2016, p. 114 e.v.

39 Vgl. Rb. Rotterdam 26 november 2002, AB 2003, 385.

Tijdschrift voor Toezicht 2016 (7) 4
doi: 10.5553/TvT/187987052016007004003

bovendien op grond van artikel 12 lid 1 AVG in beginsel in begrijpelijke taal ('clear and plain language') worden verstrekt.

De privacywetgeving lijkt de betrokkene hiermee een effectief middel in handen te geven om transparantie rondom de gebruikte big-data-analyse af te dwingen. Voor zowel de Wbp als de AVG geldt evenwel dat op de informatieplicht beperkingen mogelijk zijn, onder meer als dat nodig en evenredig is ter waarborging van een taak op het gebied van toezicht, inspectie of regelgeving (vgl. art. 43 Wbp en art. 23 AVG). Het is op voorhand niet uitgesloten dat de verantwoordelijke daarop een succesvol beroep zou kunnen doen.

De betrokkene kan een weigering om de gevraagde informatie te verstrekken voorleggen aan de rechter. Als de beslissing is genomen door een bestuursorgaan, geldt deze op de voet van artikel 45 Wbp als een besluit in de zin van de Awb waartegen bezwaar en beroep mogelijk is. In andere gevallen kan de betrokkene zich tot de civiele rechter wenden (art. 46 Wbp). Het is ook mogelijk om AP te verzoeken om op de voet van artikel 65 Wbp jo. artikel 5:32 Awb handhavend op te treden, maar in de praktijk blijkt AP vaak niet geneigd om vervolgens ook inderdaad op te treden.[40]

Als de betrokkene erin slaagt aan te tonen dat de big-data-analyse onzorgvuldig en gebrekkig is, zal dat gevolgen kunnen hebben voor de conclusies die daarop zijn gebaseerd. In het meest vergaande geval kan dat ertoe leiden dat aan het besluit de feitelijke grondslag ontbreekt: de overtreding kan bijvoorbeeld niet bewezen worden. Dat de analyse mogelijk is gebaseerd op gegevens die de toezichthouder niet had mogen hebben of gebruiken, betekent evenwel niet zonder meer dat de uitkomst van de analyse niet als bewijs zou mogen worden gebruikt als de analyse verder deugdelijk is uitgevoerd. Het is vaste rechtspraak dat het enkele feit dat bewijs mogelijk onrechtmatig is verkregen, niet zonder meer met zich brengt dat dit bewijs niet mag worden gebruikt. Dit is vaak alleen dan het geval als het bewijs is verkregen op een wijze die zo zeer indruist tegen hetgeen van een behoorlijk handelende overheid mag worden verwacht, dat het gebruik hiervan onder alle omstandigheden ontoelaatbaar moet worden geacht.[41] Het zal afhangen van de omstandigheden van het geval of dat aan de orde is. Als dat niet zo is, kan de onrechtmatigheid worden betrokken bij de bepaling van de strafmaat die dan mogelijk wordt verlaagd.

5 Ter afsluiting

We kunnen ervan uitgaan dat ook toezichthouders in toenemende mate gebruik zullen gaan maken van *big data predictive analytics* bij hun taakuitoefening. Van belang daarbij is dan dat dit gebeurt binnen de daarvoor geldende bestuursrechte-

40 Zie bijv. Rb. Gelderland 16 augustus 2016, ECLI:NL:RBGEL:2016:4553; ABRvS 19 oktober 2016, ECLI:NL:RVS:2016:2743.

41 Zie bijv. HR 1 juli 1992, NJ 1994, 621; ABRvS 12 april 2006, ECLI:NL:RVS:2006:AW1281; CBb 9 juli 2015, ECLI:NL:CBB:2015:193.

lijke en privacyrechtelijke kaders. Deze kaders hebben nog een betrekkelijk hoog abstractieniveau en de vraag is dan ook of daaraan in de handhavingspraktijk voldoende aandacht kan worden gegeven. Voor de hand ligt dat de toezichthouders die gebruikmaken van big data om te beginnen overgaan tot het opstellen van beleid en dat vastleggen in beleidsregels, waarin wordt geconcretiseerd op welke wijze en onder welke voorwaarden daarvan gebruik wordt gemaakt, hoe dat kan worden gecontroleerd en op welke wijze de belangen van rechtssubjecten worden gewaarborgd.

Maar daarbij kan het niet blijven. Van belang is dat bij het ontwerpen van informatiesystemen en de daarin toe te passen analyses ook erin wordt voorzien dat er onverminderd betekenis toekomt aan rechtsbeginselen als de onschuldpresumptie en het gelijkheidsbeginsel, het willekeursverbod, het formele en materiële gelijkheidsbeginsel enzovoort. Waar het om gaat, is dat er wordt voorzien in wat, zoals Hildebrandt suggereert, kan worden aangeduid als 'rechtsbescherming by design'.[42] Van een toezichthouder die gebruikmaakt van big-data-analyses mag worden verwacht dat hij kan aantonen dat daarmee deze rechtsbeginselen geen geweld is aangedaan. We hebben het dan over 'accountability' en ook over 'auditability'.
In het verlengde daarvan geldt dat er ook sprake moet zijn van onafhankelijk en effectief toezicht op het gebruik van big data. In dat licht is interessant dat momenteel juist bij het toezicht op de inlichtingen- en veiligheidsdiensten, waar het gebruik van big-data-analysetechnieken misschien wel het verst is ontwikkeld, wordt onderzocht onder welke randvoorwaarden vormen van geautomatiseerde surveillance mogelijk moeten zijn.[43] Het lijkt niet onaannemelijk dat deze randvoorwaarden ook relevant zijn voor toezichthouders die gebruik (willen) maken van big-data-analyses.

42 M. Hildebrandt, Data-gestuurde intelligentie in het strafrecht, in: Homo Digitalis, NJV-preadvies 2016, Deventer: Kluwer 2016, p. 218-219.

43 Commissie van Toezicht Inlichtingen- en Veiligheidsdiensten, Reactie CTIVD op conceptwetsvoorstel Wiv 20XX, Den Haag: CTIVD 2015, p. 19-21; daarover M. Hildebrandt, Data-gestuurde intelligentie in het strafrecht, in: Homo Digitalis, NJV-preadvies 2016, Deventer: Kluwer 2016, p. 219-220. <www.ctivd.nl/actueel/nieuws/2015/09/03/reactie-ctivd-conceptwetsvoorstel>.

doi: 10.5553/TvT/187987052016007004003